

DIMENSIONS OF ZASSENHAUS FILTRATION SUBQUOTIENTS OF SOME PRO- p -GROUPS

JÁN MINÁČ, MICHAEL ROGELSTAD AND NGUYỄN DUY TÂN

ABSTRACT. We compute the \mathbb{F}_p -dimension of an n -th graded piece $G_{(n)}/G_{(n+1)}$ of the Zassenhaus filtration for various finitely generated pro- p -groups G . These groups include finitely generated free pro- p -groups, Demushkin pro- p -groups and their free pro- p products. We provide a unifying principle for deriving these dimensions.

1. INTRODUCTION

Recall that for a profinite group G and a prime number p , the Zassenhaus (p -)filtration $(G_{(n)})$ of G is defined inductively by

$$G_{(1)} = G, \quad G_{(n)} = G_{([n/p])}^p \prod_{i+j=n} [G_{(i)}, G_{(j)}],$$

where $[n/p]$ is the least integer which is greater than or equal to n/p . (Here for two closed subgroups H and K of G , $[H, K]$ means the smallest closed subgroup of G containing the commutators $[x, y] = x^{-1}y^{-1}xy$, $x \in H, y \in K$. Similarly, H^p means the smallest closed subgroup of G containing the p -th powers x^p , $x \in H$.) Zassenhaus filtrations of groups were introduced in [Zas] and are now recognized as being of fundamental importance in determining the structure and properties of various types of groups. For example, in the case of absolute Galois groups, these filtrations and their subquotients have recently been investigated in [CEM, Ef1, Ef2, EM, MT, MTE]. In the case of arbitrary groups, this filtration has also been referred to as the dimension series, with the subgroups $G_{(n)}$ being called the dimension subgroups in characteristic p (see [DDMS, Chapters 11, 12]). Our goal is to develop a method for determining the \mathbb{F}_p -dimension of subquotients of the Zassenhaus filtration in the case of finitely generated pro- p groups.

Let G be a finitely generated pro- p -group. For each $n \geq 1$, we set

$$c_n(G) = \dim_{\mathbb{F}_p}(G_{(n)}/G_{(n+1)}).$$

Note that since G is finitely generated, $c_n(G)$ is finite for every $n \geq 1$ (see Section 2 for more details). We will proceed to derive an explicit formula for $c_n(G)$ for various families of groups G , including finitely generated free pro- p -groups, Demushkin groups,

JM is partially supported by the Natural Sciences and Engineering Research Council of Canada (NSERC) grant R0370A01. MR is partially supported by a CGS-D scholarship. NDT is partially supported by the National Foundation for Science and Technology Development (NAFOSTED).

and free pro-2 products of finitely many copies of the cyclic group C_2 of order 2. Galois theory provides much of the underlying motivation, as many of these groups are realizable as Galois groups of maximal p -extensions of local fields (see [De1], [Sha]) and other fields (see [EH, Proposition 1.3]). Shafarevich [Sha] demonstrated that for certain fields F not containing primitive p -th roots of unity, one could show that the Galois group of the maximal p -extension of F was a free pro- p -group simply by determining the cardinality of some of its filtration quotients.

In Remarks 3.5 (1) we show that the numbers $c_n(G)$, $n = 1, 2, \dots$, are sufficient to determine finitely generated free pro- p -groups in the family of all finitely generated pro- p -groups. In Remarks 3.5 (2) we are able to determine finitely generated free pro- p groups in the family of all Galois groups of the maximal p -extensions of fields containing a primitive p -th root of unity by just two numbers, $c_1(G)$ and $c_2(G)$. In Remarks 4.15 we show that $c_1(G)$ and $c_2(G)$ are sufficient to determine the Galois groups of the maximal 2-extensions of Pythagorean fields in two significant cases. In Subsection 4.2 we study groups G which are the free products of several copies of the cyclic group of order 2 in the category of pro-2-groups. These groups can be realized as the Galois groups of the maximal 2-extensions of Pythagorean SAP fields, and therefore they are significant in Galois theory. Each such group G contains a free pro-2-subgroup H of index 2. In Corollary 4.8 we are able to use knowledge of the numbers $c_n(G)$ and $c_n(H)$, to obtain the interesting relation $H_{(n)} = H \cap G_{(n)}$ for each $n \geq 2$. This is yet another example illustrating that the numbers $c_n(G)$ can be very useful in group theory and Galois theory.

In this paper we provide a unifying principle for deriving the dimensions $c_n(G)$ in a number of interesting cases. We observe that the formulas obtained look simple, elegant, and potentially useful. We would also like to note that when S is a finitely generated free pro- p group, a formula for $c_n(S)$ is implicitly given in [Gä], where an \mathbb{F}_p -basis for $S_{(n)}/S_{(n+1)}$ is provided.

When we interpret the groups G considered in this paper as Galois groups, our formulas lead to formulas for the order of related Galois groups. For example, if G is isomorphic to the maximal pro- p -quotient $G_F(p)$ of the absolute Galois group G_F of a field F , and if we denote by $F_{(n)}$ the fixed field of $G_F(p)_{(n)}$, then $|\text{Gal}(F_{(n)}/F)| = p^{\sum_{i=1}^{n-1} c_i(G)}$. As indicated above, these Galois groups play a fundamental role in current Galois theory. Furthermore, we observe in Sections 3 and 5 that our formulas also lead to the determination of the minimal number of topological generators of $G_{(n)}$, for G a free pro- p -group or a Demushkin pro- p -group. In fact the orders of Galois groups $\text{Gal}(F_{(n)}/F)$ are of considerable interest in current Galois theory research. In particular, in [Ef1, MT, MTE], based partially on the special cases in [EM, MS2], the Kernel Unipotent Conjecture was formulated. If this conjecture is true, we would obtain a characterization of $G_F(p)_{(n)}$, where $n \geq 3$, as the intersection of the kernels of all Galois representations $\rho: G_F(p) \rightarrow \mathbb{U}_n(\mathbb{F}_p)$. In order to prove the Kernel Unipotent Conjecture in the case when $G_F(p)$ is finitely generated, one may try to produce enough such representations. However, in order to check whether the intersection of the kernels of given representations is in fact $G_F(p)_{(n)}$, it would be useful to know $|\text{Gal}(F_{(n)}/F)|$. This strategy

resembles the previous successful strategy of Shafarevich, mentioned above. Another very interesting project in current Galois theory is to study the possible Koszul duality relating the Galois cohomology algebra $H^*(G, \mathbb{F}_p)$ to the Lie algebra $\bigoplus_{n=1}^{\infty} G_{(n)}/G_{(n+1)}$ and its universal enveloping algebra. In order to check some corollaries of this possible Koszul duality, determination of the numbers $c_n(G)$ could play an important role.

The structure of our paper is as follows: In Section 2 we discuss Hilbert-Poincaré series and provide a general formula for $c_n(G)$ (see Theorem 2.9). In Section 3 we provide an explicit formula for $c_n(G)$ when G is a free pro- p -group of finite rank. In Section 4 we treat the case when G is a free pro-2 product of finite copies of C_2 . We also show that in some significant special cases, knowledge of just $c_1(G)$ and $c_2(G)$ is sufficient to determine certain Galois groups within large families of pro-2-groups. In Section 5 we treat the case in which G is a Demushkin group. In the last section we discuss some other groups.

Acknowledgements: The first author gratefully acknowledges discussions with I. Efrat, J. Labute and A. Topaz; the latter two having provided some extra motivation for the work in this paper. All of the authors would like to thank the referee for valuable suggestions related to the exposition.

2. HILBERT-POINCARÉ SERIES

Let F be a unital commutative ring. A graded free F -module $V = \bigoplus_{i=0}^{\infty} V_n$ is called *locally finite* if $\text{rank}_F(V_n) < \infty$ for all $n \geq 0$. For such a graded free F -module V , the *Hilbert-Poincaré series* $P_V(t) \in \mathbb{Z}[[t]]$ of V is the formal power series

$$P_V(t) = \sum_{n=0}^{\infty} \text{rank}_F(V_n) t^n.$$

Let G be a finitely generated pro- p -group. It is convenient to use the completed group algebra $\mathbb{F}_p[[G]]$ of G over \mathbb{F}_p

$$\mathbb{F}_p[[G]] := \varprojlim_N \mathbb{F}_p[G/N].$$

Thus $\mathbb{F}_p[[G]]$ is the topological inverse limit of the usual group rings $\mathbb{F}_p[G/N]$, where N runs through open normal subgroups of G . A standard reference for completed group rings is [NSW, Chapter 5]. We also use the convenient references [Ko, Chapter 7] and [DDMS, Chapters 7 and 12]. We recall that $I(G) \subset \mathbb{F}_p[[G]]$ denotes the augmentation ideal of $\mathbb{F}_p[[G]]$ which is the closed two-sided ideal of $\mathbb{F}_p[[G]]$ generated by the elements $g - 1$, for $g \in G$. Thus if $\epsilon: \mathbb{F}_p[[G]] \rightarrow \mathbb{F}_p$ is the homomorphism such that $\epsilon(g) = 1$ for all $g \in G$, then $I(G) = \ker \epsilon$. We denote by $I^n(G)$ the n -th power of the augmentation ideal $I(G)$. There are two graded \mathbb{F}_p -algebras associated to G and $\mathbb{F}_p[[G]]$ respectively, which are defined by

$$\text{gr}(G) = \bigoplus_{n \geq 1} G_{(n)}/G_{(n+1)} \quad \text{and} \quad \text{gr}(\mathbb{F}_p[[G]]) = \bigoplus_{n \geq 0} I^n(G)/I^{n+1}(G).$$

Then $\text{gr}(G)$ is a restricted Lie algebra. (See [DDMS, Chapter 12].) Furthermore since G is finitely generated, the two graded algebras $\text{gr}(G)$ and $\text{gr}(\mathbb{F}_p[[G]])$ are locally finite (see [Ko, Section 7.4]). We recall that $c_n(G) = \dim_{\mathbb{F}_p} G_{(n)}/G_{(n+1)}$ and we let $a_n(G) := \dim_{\mathbb{F}_p} I^n(G)/I^{n+1}(G)$. As pointed out in [DDMS, page 312], $a_n(G) = \dim_{\mathbb{F}_p} I_0^n(G)/I_0^{n+1}(G)$, where $I_0(G)$ is the augmentation ideal of $\mathbb{F}_p[G]$ - the usual group ring of G . Thus our results below apply to this case as well. In several places we use results from discrete groups which extend in a straightforward way to pro- p -groups. We usually mention this, but in some cases we omit explicitly mentioning such a standard extension. The following theorem, Theorem 2.1, is a consequence of a beautiful theory of Jennings and Lazard [DDMS, Chapters 11 and 12] viewing the Zassenhaus filtration subgroups $G_{(n)}$ as dimension subgroups. (See also [Qu].)

Theorem 2.1 (Jennings-Lazard). *Let the notation be as above.*

- (1) *The graded algebra $\text{gr}(\mathbb{F}_p[[G]])$ is a restricted universal enveloping algebra of $\text{gr}(G)$.*
- (2) *We have*

$$(1) \quad P_{\text{gr}(\mathbb{F}_p[[G]])}(t) = \sum_{n=0}^{\infty} a_n(G) t^n = \prod_{n=1}^{\infty} \left(\frac{1 - t^{np}}{1 - t^n} \right)^{c_n(G)}.$$

Proof. (1) See [DDMS, Theorem 12.8].

(2) See [DDMS, Theorem 12.16] (see also [Er, Proposition 2.3]). \square

The following lemma is an important technical tool which allows us to derive our results in a concise way. It relies on one fundamental result of Lichtman and also on a simple, but quite remarkable formula which can be traced back to the work of Lemaire in [Le, Chapter 5].

Lemma 2.2. *Let G_1 and G_2 be two finitely generated pro- p -groups. Let $G = G_1 * G_2$ be the free product of G_1 and G_2 in the category of pro- p -groups. Then*

$$P_{\text{gr}(\mathbb{F}_p[[G]])}(t) = (P_{\text{gr}(\mathbb{F}_p[[G_1]])}^{-1}(t) + P_{\text{gr}(\mathbb{F}_p[[G_2]])}^{-1}(t) - 1)^{-1}.$$

Proof. By [Li, Theorem 1], the graded \mathbb{F}_p -algebra $\text{gr}(\mathbb{F}_p[[G]])$ is a free product (i.e., a categorical coproduct) of $\text{gr}(\mathbb{F}_p[[G_1]])$ and $\text{gr}(\mathbb{F}_p[[G_2]])$. The statement then follows from [PP, Equation (1.2), page 56]. \square

Remark 2.3. Let $G = G_1 \times G_2$ be the direct product of two finitely generated pro- p -groups G_1 and G_2 . We first observe that every commutator in G is the product of a commutator in G_1 and a commutator in G_2 , and every p -power in G is the product of a p -power in G_1 and a p -power in G_2 . Then we can check that $G_{(n)} = (G_1)_{(n)} \times (G_2)_{(n)}$, and that

$$\frac{G_{(n)}}{G_{(n+1)}} \simeq \frac{(G_1)_{(n)}}{(G_1)_{(n+1)}} \times \frac{(G_2)_{(n)}}{(G_2)_{(n+1)}}.$$

This implies that $c_n(G) = c_n(G_1) + c_n(G_2)$, and that

$$P_{\text{gr}(\mathbb{F}_p[[G]])}(t) = P_{\text{gr}(\mathbb{F}_p[[G_1]])}(t) \cdot P_{\text{gr}(\mathbb{F}_p[[G_2]])}(t).$$

In fact, since $\text{gr}(G) \simeq \text{gr}(G_1) \oplus \text{gr}(G_2)$, one can show that

$$\text{gr}(\mathbb{F}_p[[G]]) \simeq \text{gr}(\mathbb{F}_p[[G_1]]) \otimes \text{gr}(\mathbb{F}_p[[G_2]]).$$

Examples 2.4. In our examples below, d can be any natural number, and in (3), $d = 0$ is also meaningful.

- (1) If G is a free pro- p -group of rank d , then (see Section 3)

$$P_{\text{gr}(\mathbb{F}_p[[G]])}(t) = \frac{1}{1 - dt}.$$

- (2) If $G = C_p$ is a cyclic group of order p , then

$$P_{\text{gr}(\mathbb{F}_p[[G]])}(t) = 1 + t + \cdots + t^{p-1}.$$

Indeed, since $\text{gr}(C_p) = C_p$, the graded algebra $\text{gr}(\mathbb{F}_p[[G]])$, which is a universal enveloping algebra of $\text{gr}(C_p)$ by Theorem 2.1, is isomorphic to $\mathbb{F}_p[X]/(X^p)$, the preceding statement follows.

- (3) If $G = C_p * \cdots * C_p$ is a free product of $d + 1$ copies of C_p the cyclic group of order p , then

$$P_{\text{gr}(\mathbb{F}_p[[G]])}(t) = \frac{1 + t + \cdots + t^{p-1}}{1 - dt - \cdots - dt^{p-1}}.$$

This follows by induction on d , and by using (2) above, and Lemma 2.2.

- (4) If $G = \mathbb{Z}_p^d$, then

$$P_{\text{gr}(\mathbb{F}_p[[G]])}(t) = \frac{1}{(1 - t)^d}.$$

This follows from Remark 2.3 and (1) above.

- (5) If $G := \mathbb{Z}_2^d \rtimes C_2$, where $C_2 = \langle x \rangle$ and the action of C_2 on \mathbb{Z}_2^d is given by $xyx = y^{-1}$, for all $y \in \mathbb{Z}_2^d$, then (see Corollary 4.14)

$$P_{\text{gr}(\mathbb{F}_2[[G]])}(t) = \frac{1 + t}{(1 - t)^d} \prod_{i=1}^{\infty} \frac{1}{1 - t^{2i+1}}.$$

- (6) If G is a Demushkin pro- p -group of rank d , then (see Section 5)

$$P_{\text{gr}(\mathbb{F}_p[[G]])}(t) = \frac{1}{1 - dt + t^2}.$$

- (7) If G is a free product of a cyclic group of order 2 and a free pro-2-group of rank d , then

$$P_{\text{gr}(\mathbb{F}_p[[G]])}(t) = \frac{1 + t}{1 - dt - dt^2}.$$

This follows by using Lemma 2.2 and (1)-(2) above. □

Below we shall describe a general method for deriving a formula for $c_n(G)$ if we know the Hilbert-Poincaré series $P_{\text{gr}(\mathbb{F}_p[[G]])}(t)$. So we assume that we are given a power series $P(t) = 1 + \sum_{n \geq 1} a_n t^n \in \mathbb{Z}[[t]]$. We define $c_n, n = 1, 2, \dots$ by

$$P(t) = 1 + \sum_{n \geq 1} a_n t^n = \prod_{n=1}^{\infty} \left(\frac{1 - t^{np}}{1 - t^n} \right)^{c_n}.$$

We write $\log P(t) = \sum_{n \geq 1} b_n t^n$. We shall derive a formula for c_n using the values b_1, \dots, b_n . To do this, it is convenient to introduce a new auxiliary sequence w_1, w_2, \dots defined below.

Taking logarithms and using $\log\left(\frac{1}{1-t}\right) = \sum_{v=1}^{\infty} \frac{1}{v} t^v$, we obtain

$$\sum_{n=1}^{\infty} b_n t^n = \sum_{m=1}^{\infty} c_m \sum_{v=1}^{\infty} \frac{1}{v} (t^{mv} - t^{mpv}).$$

Equating the coefficients of t^n , we obtain

$$b_n = \sum_{mv=n} \frac{1}{v} c_m - \sum_{mpv=n} \frac{1}{v} c_m.$$

Hence

$$nb_n = \sum_{m|n} mc_m - \sum_{mp|n} mpc_m.$$

Recall that for two integers a and b , the symbol $a \mid b$ means that a divides b . Now we define the sequence $w_n, n = 1, 2, \dots$ by

$$w_n = \frac{1}{n} \sum_{m|n} \mu(n/m) mb_m.$$

Then by the Möbius inversion formula,

$$nb_n = \sum_{m|n} mw_m.$$

Here μ is the Möbius function: for a positive integer d ,

$$\mu(d) = \begin{cases} (-1)^r & \text{if } d \text{ is a product of } r \text{ distinct prime numbers,} \\ 0 & \text{otherwise.} \end{cases}$$

Remark 2.5. From the definition of w_n we see that

$$P(t) = 1 + \sum_{n \geq 1} a_n t^n = \prod_{n=1}^{\infty} \frac{1}{(1 - t^n)^{w_n}}.$$

Lemma 2.6. *If $(n, p) = 1$ then $c_n = w_n$.*

Proof. Assume that $(n, p) = 1$. Then we have

$$nb_n = \sum_{m|n} mc_m.$$

Hence by the Möbius inversion formula, we have

$$c_n = \frac{1}{n} \sum_{m|n} \mu(n/m) mb_m = w_n. \quad \square$$

Lemma 2.7. *If p divides n , then we have*

$$c_n = c_{n/p} + w_n.$$

Proof. We proceed by induction on n . Clearly $c_p - c_1 = \frac{pb_p - b_1}{p} = w_p$, hence the statement is true for $n = p$. Therefore we assume now that $n > p$ and $p \mid n$. We assume that the statement is true for every m such that $p \mid m \mid n$, $m \neq n$. We are going to show that the statement is also true for n .

We have

$$\begin{aligned} nb_n &= \sum_{m|n} mc_m - \sum_{pm|n} pmc_m \\ &= \sum_{m|n} mc_m - \sum_{p|m|n} mc_{m/p} \\ &= \sum_{m|n, (m,p)=1} mc_m + \sum_{p|m|n} m(c_m - c_{m/p}) \\ &= \sum_{m|n, (m,p)=1} mw_m + \sum_{p|m|n, m \neq n} mw_m + n(c_n - c_{n/p}) \\ &= \sum_{m|n, m \neq n} mw_m + n(c_n - c_{n/p}). \end{aligned}$$

Combining with

$$nb_n = \sum_{m|n} mw_m,$$

we obtain $c_n - c_{n/p} = w_n$. \square

Proposition 2.8. *If $n = p^k m$ with $(m, p) = 1$, then*

$$c_n = w_m + w_{pm} + \cdots + w_{p^k m}.$$

Proof. This follows from the above two lemmas. \square

Theorem 2.9. *Let G be a finitely generated pro- p -group. We write*

$$\log P_{\text{gr}(\mathbb{F}_p[[G]])}(t) = \sum_{n \geq 1} b_n t^n \in \mathbb{Q}[[t]],$$

and we define $w_n(G)$ by

$$w_n(G) := \frac{1}{n} \sum_{m|n} \mu(n/m) m b_m.$$

Let $n = p^k m$ with $(m, p) = 1$. Then

$$c_n(G) = w_m(G) + w_{pm}(G) + \cdots + w_{p^k m}(G).$$

Proof. This follows from Theorem 2.1 and Proposition 2.8. \square

Let G be a finitely generated pro- p -group. We write $\log P_{\text{gr}(\mathbb{F}_p[[G]])}(t) = \sum_{n \geq 1} b_n t^n$ and recall that we have defined $w_n(G)$ by

$$w_n(G) = \frac{1}{n} \sum_{m|n} \mu(n/m) m b_m.$$

At first glance the definition of w_n may look a bit artificial. One may ask whether w_n appears more naturally as the rank or dimension of some free finitely generated abelian group. Below we shall give a partial answer to this question. Recall that for a profinite group G , the descending central series (G_n) is defined inductively by

$$G_1 = G, \quad G_{n+1} = [G_n, G].$$

Let $J(G)$ be the augmentation ideal of the completed group ring $\mathbb{Z}_p[[G]]$. (Here $\mathbb{Z}_p[[G]]$ and $J(G)$ are defined similarly to $\mathbb{F}_p[[G]]$ and $I(G)$.) Then we have two graded \mathbb{Z}_p -algebras associated to G and $\mathbb{Z}_p[[G]]$ respectively which are defined by

$$\text{gr}_\gamma(G) = \bigoplus_{n \geq 1} G_n / G_{n+1} \quad \text{and} \quad \text{gr}(\mathbb{Z}_p[[G]]) = \bigoplus_{n \geq 0} J^n(G) / J^{n+1}(G).$$

Lemma 2.10. *Let G be a finitely generated pro- p -group. Assume that the graded algebra $\text{gr}_\gamma(G) = \bigoplus_{n \geq 1} G_n / G_{n+1}$ is torsion free. Let $e_n(G) = \text{rank}_{\mathbb{Z}_p} G_n / G_{n+1}$.*

- (a) *The graded algebra $\text{gr}(\mathbb{Z}_p[[G]])$ is a universal enveloping algebra of $\text{gr}_\gamma(G)$.*
- (b) *$J^n(G) / J^{n+1}(G)$ is a free module over \mathbb{Z}_p of finite rank $d_n(G)$, and*

$$P_{\text{gr}(\mathbb{Z}_p[[G]])}(t) = \sum_{n=0}^{\infty} d_n(G) t^n = \prod_{n=1}^{\infty} \frac{1}{(1 - t^n)^{e_n(G)}}.$$

Proof. (a) This follows from [Hart, Theorem 1.3]. In [Hart, Theorem 1.3], a discrete group G is considered, but an adaptation of this proof to the profinite case is straightforward.

(b) This follows from (a) and [La3, Proposition 2.5]. \square

Proposition 2.11. *Let G be a finitely generated pro- p -group. Assume that the graded algebra $\text{gr}_\gamma(G) = \bigoplus_{n \geq 1} G_n / G_{n+1}$ is torsion free. The following are equivalent.*

- (a) *$\text{rank}_{\mathbb{Z}_p} J^n(G) / J^{n+1}(G) = \dim_{\mathbb{F}_p} I^n(G) / I^{n+1}(G)$ for all $n \geq 1$.*
- (b) *$w_n(G) = \text{rank}_{\mathbb{Z}_p} G_n / G_{n+1}$ for all $n \geq 1$.*

Proof. We keep the existing notation as in Lemma 2.10.

(a) \Rightarrow (b): Assume that $\text{rank}_{\mathbb{Z}_p} J^n(G)/J^{n+1}(G) = \dim_{\mathbb{F}_p} I^n(G)/I^{n+1}(G)$ for all n . Then by Theorem 2.1, Remark 2.5 and Lemma 2.10, we have

$$P_{\text{gr}(\mathbb{F}_p[[G]])}(t) = \prod_{n=1}^{\infty} \frac{1}{(1-t^n)^{w_n(G)}} = P_{\text{gr}(\mathbb{Z}_p[[G]])}(t) = \prod_{n=1}^{\infty} \frac{1}{(1-t^n)^{e_n(G)}}.$$

Therefore $w_n(G) = e_n(G)$ for all $n \geq 1$.

(b) \Rightarrow (a): Assume that $w_n(G) = e_n(G)$ for all $n \geq 1$. Then by Theorem 2.1, Remark 2.5 and Lemma 2.10, we have

$$P_{\text{gr}(\mathbb{F}_p[[G]])}(t) = P_{\text{gr}(\mathbb{Z}_p[[G]])}(t).$$

Therefore $\text{rank}_{\mathbb{Z}_p} J^n(G)/J^{n+1}(G) = \dim_{\mathbb{F}_p} I^n(G)/I^{n+1}(G)$ for all $n \geq 1$. \square

Remark 2.12. We shall see in Sections 3 and 5, Remark 3.3 and Lemma 5.4, that both a free finitely generated pro- p -group and a Demushkin group with a relation of the form $r = [x_1, x_2] \cdots [x_{d-1}, x_d]$ satisfy the equivalent statements in Proposition 2.11.

Question 2.13. Let G be a finitely generated pro- p -group. We assume that the graded algebra $\bigoplus_{n \geq 1} G_n/G_{n+1}$ is torsion free. Is this true that

$$\text{rank}_{\mathbb{Z}_p}(G_n/G_{n+1}) = w_n(G)?$$

3. FREE PRO- p -GROUPS

Throughout this section we assume that S is a free pro- p -group on a finite set of generators x_1, \dots, x_d . We recall the Magnus homomorphism from the completed group algebra $\mathbb{F}_p[[S]]$ to the \mathbb{F}_p -algebra $\mathbb{F}_p\langle\langle X_1, \dots, X_d \rangle\rangle$ of the formal power series in d non-commuting variables X_1, \dots, X_d over \mathbb{F}_p . The homomorphism is given by

$$\psi: \mathbb{F}_p[[S]] \rightarrow \mathbb{F}_p\langle\langle X_1, \dots, X_d \rangle\rangle, x_i \mapsto 1 + X_i.$$

The \mathbb{F}_p -algebra $\mathbb{F}_p\langle\langle X_1, \dots, X_d \rangle\rangle$ is equipped with a natural valuation v given by

$$v\left(\sum a_{i_1, \dots, i_k} X_{i_1} \cdots X_{i_k}\right) = \inf\{k \mid a_{i_1, \dots, i_k} \neq 0\} \in \mathbb{Z}_{\geq 0} \cup \{\infty\},$$

making it a compact topological \mathbb{F}_p -algebra. One basic result is the following.

Lemma 3.1. *The Magnus homomorphism ψ is a (topological) isomorphism.*

Proof. See for example, [Se2, Chapter I, Proposition 7] or [Laz, Chapter 6]. \square

Corollary 3.2. *The Hilbert-Poincaré series*

$$P_{\text{gr}(\mathbb{F}_p[[S]])}(t) = \frac{1}{1-dt}.$$

Proof. Via the Magnus homomorphism, the augmentation ideal $I(S)$ is mapped to the ideal $I = (X_1, \dots, X_d)$ of $\mathbb{F}_p\langle\langle X_1, \dots, X_d \rangle\rangle$. Hence

$$a_n(S) := \dim_{\mathbb{F}_p}(I^n(S)/I^{n+1}(S)) = \dim_{\mathbb{F}_p}(I^n/I^{n+1}),$$

which is equal to the number of non-commutative monomials of degree n in d variables X_1, \dots, X_n . Hence $a_n(S) = d^n$. The statement then follows. \square

We define $w_n(S)$ by

$$w_n(S) = \frac{1}{n} \sum_{m|n} \mu(m) d^{n/m}.$$

Remark 3.3. Let (S_n) be the lower central series of S . Then by Witt's result, S_n/S_{n+1} is a free \mathbb{Z}_p -module of finite rank $w_n(S)$.

Theorem 2.9 immediately implies the following result.

Proposition 3.4. *If $n = p^k m$ with $(m, p) = 1$, then*

$$c_n(S) = w_m(S) + w_{pm}(S) + \dots + w_{p^k m}(S).$$

Remarks 3.5. (1) If a finitely generated pro- p -group G has Hilbert-Poincaré series of a finitely generated free pro- p -group, then G is itself free. In other words, if $P_{\text{gr}(\mathbb{F}_p[[G]])}(t) = \frac{1}{1-dt}$, then G is free of rank d . Indeed, we first have $c_1(G) = w_1(G) = d$, which is equal to the minimal number of topological generators of G . Hence there exists a minimal presentation of G :

$$1 \rightarrow R \rightarrow S \rightarrow G \rightarrow 1,$$

where S is a free pro- p -group of rank d . We then have $c_n(G) = c_n(S)$ for all $n \geq 1$. Hence $|S/S_{(n)}| = |G/G_{(n)}|$ for all $n \geq 1$. Thus the natural epimorphism

$$S/S_{(n)} \twoheadrightarrow G/G_{(n)}$$

is in fact an isomorphism. This implies that $R \subseteq S_{(n)}$ for all $n \geq 1$. Therefore by [Ko, Theorem 7.11], $R = 1$ and hence $S \simeq G$.

(2) Let G be a finitely generated pro- p -group. In the case in which G is realizable as the Galois group of a maximal p -extension of a field F containing a primitive p -th root of unity, it is noteworthy to point out that if $c_1(G) = c_1(S)$ and $c_2(G) = c_2(S)$ for some finitely generated free pro- p -group S , then G is in fact isomorphic to S . Indeed, as $c_1(S) = c_1(G)$ we have a short exact sequence

$$1 \rightarrow R \rightarrow S \xrightarrow{\pi} G \rightarrow 1.$$

Since $c_1(S) = c_1(G)$ and $c_2(S) = c_2(G)$, we see that $|S/S_{(3)}| = |G/G_{(3)}|$. Thus the natural epimorphism

$$S/S_{(3)} \twoheadrightarrow G/G_{(3)}$$

is in fact an isomorphism. Hence by [EM, Theorem C] (see also [CEM, Theorem D] for the case $p = 2$) we see that $\pi: S \rightarrow G$ is an isomorphism.

In Corollary 3.7 relying on Lemma 3.6 below, we obtain an interesting purely group-theoretical corollary of our formula for $c_n(S)$. For each positive integer n , let $\mathbb{U}_{n+1}(\mathbb{F}_p)$ be the group of all upper-triangular unipotent $(n+1) \times (n+1)$ -matrices with entries in \mathbb{F}_p .

Lemma 3.6. *Let n be a positive integer. If $\mathbb{U}_{n+1}(\mathbb{F}_p)_{(n)} = 1$, then $c_n(S) = 0$ for every free pro- p -group S .*

Proof. Let S be a free pro- p -group. Assume that $\mathbb{U}_{n+1}(\mathbb{F}_p)_{(n)} = 1$. Then for any (continuous) representation $\rho : S \rightarrow \mathbb{U}_{n+1}(\mathbb{F}_p)$, we have $\rho(S_{(n)}) \subseteq \mathbb{U}_{n+1}(\mathbb{F}_p)_{(n)} = 1$. Hence

$$S_{(n+1)} \subseteq S_{(n)} \subseteq \bigcap \ker(\rho : S \rightarrow \mathbb{U}_{n+1}(\mathbb{F}_p)),$$

where ρ runs over the set of all representations (continuous homomorphisms) $S \rightarrow \mathbb{U}_{n+1}(\mathbb{F}_p)$. On the other hand, we know that the Kernel Unipotent Conjecture is true for S (see [Ef1], and also [Ef2], [MT]). This means that we have

$$S_{(n+1)} = \bigcap \ker(\rho : S \rightarrow \mathbb{U}_{n+1}(\mathbb{F}_p)).$$

Therefore, $S_{(n+1)} = S_{(n)}$, i.e., $c_n(S) = 0$, as desired. \square

Corollary 3.7. *Let n be a positive integer. Then $\mathbb{U}_{n+1}(\mathbb{F}_p)_{(n)} \simeq \mathbb{F}_p$ and*

$$n = \max\{h \mid \mathbb{U}_{n+1}(\mathbb{F}_p)_{(h)} \neq 1\}.$$

Proof. We first observe that if S is a free pro- p -group of rank $d > 1$, then all numbers $w_n(S)$, $n = 1, 2, \dots$, are positive. Therefore from Proposition 3.4 we see that $c_n(S) \neq 0$ for all $n \in \mathbb{N}$. Hence by Lemma 3.6, $\mathbb{U}_{(n+1)}(\mathbb{F}_p)_{(n)} \neq 1$.

On the other hand, it is well-known that $\mathbb{U}_{n+1}(\mathbb{F}_p)_{(n+1)} = 1$. Hence $\mathbb{U}_{n+1}(\mathbb{F}_p)_{(n)} \subseteq Z(\mathbb{U}_{n+1}(\mathbb{F}_p)) \simeq \mathbb{F}_p$, where $Z(\mathbb{U}_{n+1}(\mathbb{F}_p))$ is the center of $\mathbb{U}_{n+1}(\mathbb{F}_p)$. Therefore

$$\mathbb{U}_{n+1}(\mathbb{F}_p)_{(n)} = Z(\mathbb{U}_{n+1}(\mathbb{F}_p)) \simeq \mathbb{F}_p,$$

and the second assertion is also clear. \square

Example 3.8. Let S be a free pro- p -group of finite rank d . We have

$$\begin{aligned} c_1(S) &= d, \\ c_2(S) &= \begin{cases} \frac{d^2-d}{2} & \text{if } p \neq 2, \\ \frac{d^2+d}{2} & \text{if } p = 2, \end{cases} \\ c_3(S) &= \begin{cases} \frac{d^3-d}{3} & \text{if } p \neq 3, \\ \frac{d^3+2d}{3} & \text{if } p = 3, \end{cases} \\ c_4(S) &= \begin{cases} \frac{d^4-d^2}{4} & \text{if } p \neq 2, \\ \frac{d^4+d^2+2d}{4} & \text{if } p = 2, \end{cases} \\ c_5(S) &= \begin{cases} \frac{d^5-d}{5} & \text{if } p \neq 5, \\ \frac{d^5+4d}{5} & \text{if } p = 5. \end{cases} \end{aligned}$$

Observe that our numbers $c_n(S)$, $n = 1, 2, \dots$, also detect the minimal numbers of generators of $S_{(n)}$. Indeed by the pro- p -version of Schreier's formula for each open subgroup

T of S , we have the following expression for the minimal number of generators $d(T)$ of T :

$$d(T) = [S : T](d(S) - 1) + 1.$$

Therefore

$$d_n(S) := d(S_{(n)}) = p^{\sum_{i=1}^{n-1} c_i(S)}(d - 1) + 1.$$

Next we are going to give an explicit \mathbb{F}_p -basis for $S_{(n)}/S_{(n+1)}$, for each n . We shall first recall a definition of Hall commutators of weight n and their linear order. This was originally introduced by M. Hall in [Ha, Section 4] (see also [Vo, Definition 2.3]).

Definition 3.9. The set C_n of Hall commutators of weight n together with a total order $<$ is inductively defined as follows:

- (1) $C_1 = \{x_1, \dots, x_d\}$ with the ordering $x_1 > \dots > x_d$.
- (2) Assume $n > 1$ and that we have defined Hall commutators and their ordering for all weights $< n$. Then C_n is the set of all commutators $[c_1, c_2]$ where $c_1 \in C_{n_1}, c_2 \in C_{n_2}$ such that $n_1 + n_2 = n$, $c_1 > c_2$ and if $c_1 = [c_3, c_4]$ then we also require that $c_2 \geq c_4$. The set C_n is ordered lexicographically, i.e., $[c_1, c_2] < [c'_1, c'_2]$ if and only if $c_1 < c'_1$, or $c_1 = c'_1$ and $c_2 < c'_2$. Finally commutators of weight n are greater than all commutators of smaller weight.

The following theorem was proved by M. Hall in the discrete case. The extension of his theorem to the pro- p case is straightforward.

Theorem 3.10 ([Ha, Theorem 4.1]). *The Hall commutators of weight n represent a basis of S_n/S_{n+1} as a free \mathbb{Z}_p -module.*

In particular $w_n(S) = |C_n|$.

The following theorem is due to Lazard (see [DDMS, Theorem 11.2]).

Theorem 3.11 (Lazard). *For each n , one has*

$$G_{(n)} = \prod_{ip^j \geq n} G_i^{p^j}.$$

Corollary 3.12. *Let us write $n = p^k m$ with $(m, p) = 1$. Then a basis of the \mathbb{F}_p -vector space $S_{(n)}/S_{(n+1)}$ can be represented by the following set*

$$C_m^{p^k} \sqcup C_{pm}^{p^{k-1}} \sqcup \dots \sqcup C_{p^{k-1}m}^p \sqcup C_n.$$

Proof. By Lazard's theorem, we can check that the above set defines a set of generators for the \mathbb{F}_p -vector space $S_{(n)}/S_{(n+1)}$. Now by Proposition 3.4 and by a counting argument, we see that this set defines a basis for the \mathbb{F}_p -vector space $S_{(n)}/S_{(n+1)}$. \square

4. FREE PRODUCTS OF A FINITE NUMBER OF CYCLIC GROUPS OF ORDER 2

4.1. Free products of finitely many cyclic groups of order 2. Let d be a non-negative integer. Let $G = C_2 * \cdots * C_2$ be a free product in the category of pro-2-groups of $d + 1$ copies of C_2 , where C_2 is the group of order 2.

In this section we shall consider Pythagorean fields. A field F is said to be Pythagorean if each finite sum of squares in F is again a square in F . A Pythagorean field is called a formally real field if -1 is not a square. Pythagorean fields play an important role in Galois theory, real algebraic geometry and the algebraic theory of quadratic forms. We refer a reader to a beautiful exposition of related topics in [Lam].

Let us recall that a formally real Pythagorean field K with $|K^\times / (K^\times)^2| = 2^{d+1}$ is called an SAP field if K admits exactly $d + 1$ orderings. These SAP fields form an interesting and well investigated family of fields. (See [Lam, Chapter 17].)

Theorem 4.1. *Let F be a field with $|F^\times / (F^\times)^2| = 2^{d+1}$. Then F is an SAP field if and only if $G_F(2)$ is isomorphic to $G = C_2 * \cdots * C_2$, the free product of $d + 1$ copies of C_2 .*

Proof. The "only if" part follows from [Mi].

We now prove the "if" part. Suppose that $G_F(2)$ is isomorphic to $C_2 * \cdots * C_2$ ($d + 1$ copies of C_2). Then F is formally real Pythagorean, and $|F^\times / (F^\times)^2| = 2^{d+1}$. Now we pick any SAP field K which has exactly $d + 1$ orderings. From the "only if" part, we see that $G_F(2) \simeq G_K(2)$. In particular, $G_F(2)/G_F(2)_{(3)} \simeq G_K(2)/G_K(2)_{(3)}$. Then [MS2, Theorem 3.8] implies that the Witt ring WF of F is isomorphic to the Witt ring WK of K . We know that for a Pythagorean field L , the Witt ring WL of L determines the space of orderings X_L of L . Hence the space of orderings of F is isomorphic to the space of orderings of K . In particular F admits exactly $d + 1$ orderings. Therefore F is an SAP field. \square

Corollary 4.2. *Let F be any Pythagorean field, and let K be an SAP field. Assume that $|F^\times / (F^\times)^2| = |K^\times / (K^\times)^2| = 2^{d+1}$. Then there exists an epimorphism $G_K(2) \simeq C_2 * \cdots * C_2 \twoheadrightarrow G_F(2)$.*

Proof. By [Lam, Remark 17.5], F has at least $d + 1$ orderings, and we can choose $d + 1$ involutions $\sigma_1, \dots, \sigma_{d+1}$ in $G = G_F(2)$ such that $\sigma_1, \dots, \sigma_{d+1}$ minimally generate $G_F(2)$. The statement then follows from the previous theorem. \square

Our treatment below is purely group-theoretical. However the group G plays an important role as the maximal pro-2 quotient of the absolute Galois group of SAP fields. (We refer the interested reader to [Har], [Mi].) Also it is interesting to observe that if $G = C_2 * \cdots * C_2$ is the Galois group as above, then G is already determined by its quotient $G/G_{(3)}$. (See also Remarks 4.15 for closely related observations.) More precisely, assume that H is another pro-2-group which is realizable as the Galois group of the maximal 2-extension of a field F , and that $H/H_{(3)} \simeq G/G_{(3)}$, then $H \simeq G$. (See [MS1, MS2, Mi].)

The Hilbert-Poincaré series of $\text{gr}(\mathbb{F}_2[[G]])$ is

$$P_{\text{gr}(\mathbb{F}_2[[G]])}(t) = \frac{1+t}{1-dt}.$$

Remark 4.3. Since the cohomology algebra $H^*(C_2, \mathbb{F}_2)$ is isomorphic to $\mathbb{F}_2[X]$, the polynomial algebra in one variable X over \mathbb{F}_2 , we have

$$P_{H^*(G, \mathbb{F}_2)}(t) = \sum_{n=0}^{\infty} \dim_{\mathbb{F}_2}(H^n(G, \mathbb{F}_2))t^n = 1 + (d+1)t + (d+1)t^2 + \cdots = \frac{1+dt}{1-t}$$

by [NSW, Theorems 4.1.4-4.1.5]. Therefore, we have

$$P_{H^*(G, \mathbb{F}_2)}(t)P_{\text{gr}(\mathbb{F}_2[[G]])}(-t) = 1.$$

This is not a coincidence. One can show that the cohomology algebra $H^*(G, \mathbb{F}_2)$ is Koszul and that $\text{gr}(\mathbb{F}_2[[G]])$ is its Koszul dual. The above equality is just a special case of the well-known relation between the two Hilbert-Poincaré series of a Koszul algebra and its dual (see [PP, Corollary 2.2]). \square

We have

$$\log P_{\text{gr}(\mathbb{F}_2[[G]])}(t) = \log\left(\frac{1}{1-dt}\right) - \log\left(\frac{1}{1+t}\right) = \sum_{n \geq 1} \frac{1}{n}(d^n - (-1)^n)t^n.$$

Now we define the sequence $w_n(G), n = 1, 2, \dots$ by

$$w_n(G) = \frac{1}{n} \sum_{m|n} \mu(n/m)(d^m - (-1)^m).$$

Proposition 4.4. *If $n = 2^k m$ with $(m, 2) = 1$, then*

$$c_n(G) = w_m(G) + w_{2m}(G) + \cdots + w_{2^k m}(G). \quad \square$$

4.2. Free products of the cyclic group of order 2 as semidirect products. Let $G = C_2 * \cdots * C_2$ be a free product in the category of pro-2-groups of $d+1$ copies of C_2 . In this subsection we shall show that G is isomorphic to a semidirect product $H \rtimes C_2$ of a free pro-2-group H and C_2 . We also provide a relation between $G_{(n)}$ and $H_{(n)}$.

We define the numbers $\epsilon_n, n = 1, 2, \dots$ by

$$\epsilon_n = \frac{1}{n} \sum_{m|n} \mu(n/m)(-1)^m,$$

i.e., by the Möbius inversion formula,

$$(*) \quad (-1)^n = \sum_{m|n} m \epsilon_m.$$

Lemma 4.5. *We have $\epsilon_1 = -1, \epsilon_2 = 1$ and $\epsilon_n = 0$ for $n \geq 3$.*

Proof. The equation (*) determines ϵ_n , $n \in \mathbb{N}$, uniquely. But $\epsilon_1 = -1$, $\epsilon_2 = 1$ and $\epsilon_n = 0$ for $n \geq 3$ work as for these numbers

$$\sum_{m|n} m\epsilon_m = \begin{cases} -1 & \text{if } n \text{ is odd,} \\ -1 + 2 = 1 & \text{if } n \text{ is even.} \quad \square \end{cases}$$

Let us write

$$G = C_2 * C_2 * \cdots * C_2 = \langle x_0 \mid x_0^2 \rangle * \langle x_1 \mid x_1^2 \rangle * \cdots * \langle x_d \mid x_d^2 \rangle.$$

For ease of notation, we consider x_0, x_1, \dots, x_d as elements of G . We consider a continuous homomorphism $\varphi : G \rightarrow C_2 = \langle x \mid x^2 \rangle$ defined by $x_i \mapsto x$ for all $i = 0, 1, \dots, d$. For each $i = 1, \dots, d$, we set $y_i = x_0 x_i \in G$ and let H be the closed subgroup of G generated by y_1, \dots, y_d .

Lemma 4.6. *Let the notation be as above.*

- (1) $\ker \varphi = H$.
- (2) H is a free pro-2-group of rank d .
- (3) We have $G \simeq H \rtimes C_2$, where the action of C_2 on H is given by $xy_i x = y_i^{-1}$.

Proof. (1) Clearly $y_i \in \ker \varphi$, hence $H \subseteq \ker \varphi$. Now consider any element $\gamma \in \ker \varphi$. Then for each open neighborhood U of γ in G , there exists an element $g = x_{i_1} \cdots x_{i_r} \in U$, $i_1, \dots, i_r \in \{1, \dots, d\}$ such that $1 = \varphi(g) = x^r$. Hence $r = 2s$ is even. Since $x_0 y_i x_0 = y_i^{-1}$, we obtain

$$g = x_0 y_{i_1} \cdots x_0 y_{i_r} = y_{i_1}^{-1} y_{i_2} \cdots y_{i_{r-1}}^{-1} y_{i_r}.$$

Thus $g \in H$. Therefore $\gamma \in H$ and $H = \ker \varphi$.

(2) By profinite analogue of the well known Kurosch's subgroup theorem in the theory of free products of discrete groups due to E. Binz, J. Neukirch and G. Wenzel explained in [NSW, Theorem 4.2.1 and Remarks below this Theorem], we see that H is indeed a free pro-2-group of rank d .

(3) This follows by observing that $\psi : C_2 = \langle x \mid x^2 \rangle \rightarrow G$ which maps \bar{x} to x_1 , is a section of φ . \square

The following proposition and corollary are remarkable properties of the pair $\{H, G\}$.

Proposition 4.7. *We have $c_1(H) = d = c_1(G) - 1$ and $c_n(H) = c_n(G)$ for all $n \geq 2$.*

Proof. It is clear that $c_1(H) = w_1(H) = d$ and $c_1(G) = w_1(G) = d + 1$. Hence $c_1(H) = d = c_1(G) - 1$. We shall show that $c_n(H) = c_n(G)$ for any $n \geq 2$.

We note that

$$w_n(H) - w_n(G) = \frac{1}{n} \sum_{m|d} \mu(n/m) (-1)^m = \epsilon_n.$$

By Lemma 4.5, one has $w_2(H) = w_2(G) + 1$ and $w_n(H) = w_n(G)$ for every $n \geq 3$.

If $n > 1$ is odd, then

$$c_n(H) = w_n(H) = w_n(G) = c_n(G).$$

If n is even, then by writing $n = 2^k m$ with m odd, we have

$$\begin{aligned} c_n(H) &= w_m(H) + w_{2m}(H) + w_{4m}(H) + \cdots + w_{2^k m}(H) \\ &= w_m(G) + w_{2m}(G) + w_{4m}(G) + \cdots + w_{2^k m}(G) = c_n(G). \end{aligned}$$

(Note that we always have $w_m(H) + w_{2m}(H) = w_m(G) + w_{2m}(G)$ for every $m \geq 1$ odd.) \square

Corollary 4.8. *Let $n \geq 2$ be an integer.*

- (1) $H_{(n)} = H \cap G_{(n)}$.
- (2) $G/G_{(n)} \simeq H/H_{(n)} \rtimes C_2$, where the action of C_2 on $H/H_{(n)}$ is given by $\bar{x}\bar{y}_i\bar{x} = \bar{y}_i^{-1}$.

Proof. (1) Clearly $H_{(n)} \subseteq H \cap G_{(n)}$. We proceed by induction on n to show that $H_{(n)} = H \cap G_{(n)}$. First consider the case $n = 2$. We have an exact sequence

$$1 \rightarrow H/H \cap G_{(2)} \rightarrow G/G_{(2)} \rightarrow C_2 \rightarrow 1.$$

This implies that $[H : H \cap G_{(2)}] = [G : G_{(2)}]/2 = 2^d = [H : H_{(2)}]$. Hence $H_{(2)} = H \cap G_{(2)}$. Assume that $H_{(n)} = H \cap G_{(n)}$ for some $n \geq 2$. Then from the exact sequence

$$1 \rightarrow H/H \cap G_{(n)} \rightarrow G/G_{(n)} \rightarrow C_2 \rightarrow 1,$$

we obtain $[H : H_{(n)}] = [H : H \cap G_{(n)}] = [G : G_{(n)}]/2$. From a similar exact sequence we obtain

$$\begin{aligned} [H : H \cap G_{(n+1)}] &= \frac{1}{2}[G : G_{(n+1)}] = \frac{1}{2}[G : G_n][G_{(n)} : G_{(n+1)}] \\ &= [H : H_{(n)}][H_{(n)} : H_{(n+1)}] = [H : H_{(n+1)}]. \end{aligned}$$

Here the equality $[G_{(n)} : G_{(n+1)}] = [H_{(n)} : H_{(n+1)}]$ follows from Proposition 4.7. Therefore $H_{(n+1)} = H \cap G_{(n+1)}$.

(2) This follows from (1). \square

4.3. Another semidirect product. In this subsection we consider an example in which G is the semidirect product $G := \mathbb{Z}_2^d \rtimes C_2 = H \rtimes \langle x \rangle$, where the action of C_2 on $H := \mathbb{Z}_2^d$ is given by $xyx = y^{-1}$, for all $y \in H$. This group G is realizable as the maximal pro-2-quotient of the absolute Galois group of a superpythagorean field. Recall that a formally real Pythagorean field F with $|F^\times / (F^\times)^2| = 2^{d+1} < \infty$ is called a superpythagorean field if F admits exactly 2^d orderings.

Proposition 4.9. *Let F be a Pythagorean field with $|F^\times / (F^\times)^2| = 2^{d+1}$. Then there exists an epimorphism $G_F(2) \twoheadrightarrow G = \mathbb{Z}_2^d \rtimes C_2$.*

Proof. We choose any ordering P in F and an \mathbb{F}_2 -basis $[a_1], \dots, [a_d]$ of $P/(F^\times)^2$. By [Be1] we know that there exists a field E , the Euclidean closure of F with respect to P such that $F(2) = E(\sqrt{-1})$, E is a formally real field and $(E^\times)^2 \cap F^\times = P$. We can pick for each a_i as above, a sequence

$$\sqrt{a_i}, \sqrt[4]{a_i}, \dots, \sqrt[2^n]{a_i}, \dots,$$

such that all $\sqrt[n]{a_i}$ are in E^\times . Indeed, by induction on n we may assume that $\sqrt[n]{a_i}$ is in E^\times . Then we can pick $\sqrt[n+1]{a_i}$ in $(E^\times)^2$ because $E^\times = (E^\times)^2 \cup -(E^\times)^2$. We set

$$\tilde{M} := \bigcup_{n=1}^{\infty} F(\sqrt[n]{a_1}, \dots, \sqrt[n]{a_d}).$$

Then \tilde{M} is formally real since \tilde{M} is a subfield of E . We recall that for each $n \in \mathbb{N}$, $F(\sqrt{-1})$ contains a primitive 2^n -th root of unity ζ_{2^n} . (See [Be2, Chapter II, Theorem 8].) We may also assume that $\zeta_{2^{n+1}}^2 = \zeta_{2^n}$. We set $M := \tilde{M}(\sqrt{-1})$. Then M/F is a Galois extension.

We show that $\text{Gal}(M/F\sqrt{-1})$ is isomorphic to \mathbb{Z}_2^d . This follows from Kummer theory. In fact, let τ_1, \dots, τ_d be elements in $\text{Gal}(M/F(\sqrt{-1}))$ such that for each $i = 1, \dots, d$, one has

$$\tau_i(\sqrt[n]{a_i}) = \zeta_{2^n} \sqrt[n]{a_i}, \text{ and } \tau_i(\sqrt[n]{a_j}) = \sqrt[n]{a_j} \forall j \neq i.$$

Then $\text{Gal}(M/F(\sqrt{-1})) = (\prod_{i=1}^d \langle \tau_i \rangle) \simeq \mathbb{Z}_2^d$.

We observe that the restriction of a nontrivial element of $\text{Gal}(E(\sqrt{-1})/E)$ to M gives us a nontrivial element $\sigma \in \text{Gal}(M/\tilde{M})$. Thus we have a splitting

$$\text{Gal}(M/F) \simeq \text{Gal}(M/F\sqrt{-1}) \rtimes \langle \sigma \rangle,$$

where $\langle \sigma \rangle \simeq C_2$, and the action of C_2 on $\text{Gal}(M/F\sqrt{-1})$ is by involution.

The natural projection

$$G_F(2) = \text{Gal}(F(2)/F) \rightarrow \text{Gal}(M/F) \simeq \mathbb{Z}_2^d \rtimes C_2$$

gives the desired epimorphism. \square

Corollary 4.10. *Let F be a field with $|F^\times / (F^\times)^2| = 2^{d+1}$. Then F is a superpythagorean field if and only if $G_F(2)$ is isomorphic to the group $G = \mathbb{Z}_2^d \rtimes C_2$.*

Proof. Assume that F is a superpythagorean field with $|F^\times / (F^\times)^2| = 2^{d+1}$. Let the notation be as in the previous proposition. Then $\text{Gal}(M/F) \simeq G = \mathbb{Z}_2^d \rtimes C_2$. On the other hand, from [Wa, Example 3.8, (ii)] (see also [Be2, Chapter III, Theorem 1]), we know that $\text{Gal}(M/F)$ is equal to $G_F(2)$. Hence $G_F(2) \simeq \mathbb{Z}_2^d \rtimes C_2$.

The converse direction is proved in a similar fashion to the proof of the "if" part in Theorem 4.1. \square

Corollary 4.11. *Let F be any Pythagorean field, and let K be a superpythagorean field. Assume that $|F^\times / (F^\times)^2| = |K^\times / (K^\times)^2| = 2^{d+1}$. Then there exists an epimorphism $G_F(2) \twoheadrightarrow G_K(2) \simeq \mathbb{Z}_2^d \rtimes C_2$.*

Proof. This follows from the previous theorem and corollary. \square

Lemma 4.12. *Let $G = H \rtimes \langle x \rangle = \mathbb{Z}_2^d \rtimes C_2$ be as above. Let $n \geq 2$ be an integer, and let $s = \lceil \log_2 n \rceil$. Then $G_{(n)} = H^{2^s}$.*

Proof. We proceed by induction on n . We first observe that $[y, x] = y^{-1}x^{-1}yx = (y^{-1})^2$ and $(yx)^2 = y^2$, for every $y \in H$. Hence

$$G_{(2)} = G^2[G, G] = G^2 = H^2.$$

The lemma is true for $n = 2$. We assume that the lemma is true for j with $2 \leq j < n$. Then

$$\begin{aligned} G_{(n)} &= G_{([n/2])}^2 \prod_{i+j=n} [G_{(i)}, G_{(j)}] \\ &= G_{([n/2])}^2 [G, G_{(n-1)}] \\ &= (H^{2^{s-1}})^2 = H^{2^s}. \end{aligned}$$

Here we use that $G_{n-1} \subseteq H^{2^{s-1}}$, and hence $[G, G_{(n-1)}] \subseteq H^{2^s}$. \square

An immediate consequence of the above lemma is the following result.

Corollary 4.13. *Let $n \geq 2$ be an integer. We have*

$$c_n(G) = \begin{cases} d+1 & \text{if } n = 1, \\ d & \text{if } n = 2^s \text{ for some } 1 \leq s \in \mathbb{Z}, \\ 1 & \text{if } n \text{ is not a power of 2.} \end{cases}$$

Corollary 4.14. *We have*

$$P_{\text{gr}(\mathbb{F}_2[[G]])}(t) = \frac{1+t}{(1-t)^d} \prod_{i=1}^{\infty} \frac{1}{1-t^{2i+1}}.$$

Proof. We write $\log P_{\text{gr}(\mathbb{F}_2[[G]])} = \sum_{n \geq 1} b_n(G) t^n$, and let

$$w_n(G) = \frac{1}{n} \sum_{m|n} \mu(n/m) m b_m(G).$$

By Lemma 2.6, if n is odd then $w_n(G) = c_n(G)$. In particular, $w_1(G) = c_1(G) = d+1$, and $w_{2i+1}(G) = c_{2i+1}(G) = 1$ for $i \geq 1$.

By Lemma 2.7, $w_2(G) = c_2(G) - c_1(G) = d - (d+1) = -1$.

We claim that $w_n(G) = 0$ if n is even and $n \geq 4$. Indeed, if $n = 2^s$ with $s \geq 2$, then by Lemma 2.7,

$$w_{2^s}(G) = c_{2^s}(G) - c_{2^{s-1}}(G) = d - d = 0.$$

Now if $n = 2m$, where m is not a power of 2, then also by Lemma 2.7,

$$w_{2m}(G) = c_{2m}(G) - c_m(G) = 1 - 1 = 0.$$

The corollary then follows from Remark 2.5. \square

Remarks 4.15. It is an interesting fact that $c_1(G)$ and $c_2(G)$ can be sufficient in determining G itself within some large families of pro- p -groups. We mentioned an example in Remarks 3.5 (2). Here are two other instances.

(1) Suppose that K is an SAP field with $|K^\times / (K^\times)^2| = 2^{d+1}$. Then $G_K(2) = C_2 * \cdots * C_2$, the free product of $d + 1$ copies of C_2 . By Proposition 4.4, one has

$$c_1(G_K(2)) = d + 1 \text{ and } c_2(G_K(2)) = \frac{d(d+1)}{2}.$$

Now let F be a formally real Pythagorean field F with $|F^\times / (F^\times)^2| < \infty$. We assume that $c_1(G_F(2)) = d + 1$ and that $c_2(G_F(2)) = d(d+1)/2$ for some integer $d \geq 0$. Then we claim that F is an SAP field with exactly $d + 1$ orderings. So, quite remarkably, within the family of formally real Pythagorean fields with finitely many square classes, the numbers $c_1(G_F(2))$ and $c_2(G_F(2))$ above suffice to characterize SAP fields F . We shall now prove this claim. Because $c_1(G_F(2)) = d + 1$, we see that $G_F(2)$ has $d + 1$ minimal generators, and therefore $|F^\times / (F^\times)^2| = 2^{d+1}$. We pick any SAP field K with $|K^\times / (K^\times)^2| = 2^{d+1}$. By Corollary 4.2, there exists an epimorphism $\varphi: G_K(2) \twoheadrightarrow G_F(2)$. We have

$$\begin{aligned} |G_K(2)/G_K(2)_{(3)}| &= c_1(G_K(2)) + c_2(G_K(2)) \\ &= d + \frac{d(d+1)}{2} \\ &= c_1(G_F(2)) + c_2(G_F(2)) \\ &= |G_F(2)/G_F(2)_{(3)}|. \end{aligned}$$

This implies that the induced epimorphism $G_K(2)/G_K(2)_{(3)} \twoheadrightarrow G_F(2)/G_F(2)_{(3)}$ is an isomorphism. By [CEM, Theorem D], $\varphi: G_K(2) \rightarrow G_F(2)$ is an isomorphism. This implies that F is a SAP field by Theorem 4.1.

(2) Suppose that K is a superpythagorean field with $|K^\times / (K^\times)^2| = 2^{d+1} < \infty$. By Corollary 4.13, one has

$$c_1(G_K(2)) = d + 1 \text{ and } c_2(G_K(2)) = d.$$

Now let F be a formally real Pythagorean field F with $|F^\times / (F^\times)^2| < \infty$. We assume that $c_1(G_F(2)) = d + 1$, $c_2(G_F(2)) = d$ for some integer $d \geq 0$. Then we claim that F is a superpythagorean field. So within the family of formally real Pythagorean fields with finitely many square classes, the numbers $c_1(G_F(2))$ and $c_2(G_F(2))$ above, also suffice to characterize superpythagorean fields F . We shall now prove this claim. We pick any superpythagorean field K with $|K^\times / (K^\times)^2| = 2^{d+1}$. By Corollary 4.14, we have an epimorphism $\varphi: G_F(2) \twoheadrightarrow G_K(2)$. We have

$$\begin{aligned} |G_F(2)/G_F(2)_{(3)}| &= c_1(G_F(2)) + c_2(G_F(2)) \\ &= d + 1 + d \\ &= c_1(G_K(2)) + c_2(G_K(2)) \\ &= |G_K(2)/G_K(2)_{(3)}|. \end{aligned}$$

This implies that the induced epimorphism $G_F(2)/G_F(2)_{(3)} \twoheadrightarrow G_K(2)/G_K(2)_{(3)}$ is an isomorphism. By [CEM, Theorem D], $\varphi: G_F(2) \rightarrow G_K(2)$ is an isomorphism. This implies that F is a superpythagorean field by Corollary 4.10. \square

5. DEMUSHKIN GROUPS

Recall that a pro- p -group G is said to be a Demushkin group if

- (1) $\dim_{\mathbb{F}_p} H^1(G, \mathbb{F}_p) < \infty$,
- (2) $\dim_{\mathbb{F}_p} H^2(G, \mathbb{F}_p) = 1$,
- (3) the cup product $H^1(G, \mathbb{F}_p) \times H^1(G, \mathbb{F}_p) \rightarrow H^2(G, \mathbb{F}_p)$ is a non-degenerate bilinear form.

By the work of [De1, De2], [Se1] and [La1], we now have a complete classification of Demushkin groups.

Let G be a Demushkin group of rank $d = \dim_{\mathbb{F}_p} H^1(G, \mathbb{F}_p)$. Let $c_n = c_n(G)$. Then by [La3, Theorem 5.1 (g)] (see also [Fo, Gä, LM]), we have the Hilbert-Poincaré series

$$P_{\text{gr}(\mathbb{F}_p[[G]])}(t) = \frac{1}{1 - dt + t^2}.$$

We write $1 - dt + t^2 = (1 - at)(1 - bt)$ so that $a + b = d$ and $ab = 1$. Then

$$\log P_{\text{gr}(\mathbb{F}_p[[G]])}(t) = \log\left(\frac{1}{1 - at}\right) + \log\left(\frac{1}{1 - bt}\right) = \sum_{n \geq 1} \frac{1}{n} (a^n + b^n).$$

We define the sequence $w_n(G), n = 1, 2, \dots$ by

$$w_n(G) = \frac{1}{n} \sum_{m|n} \mu(m) (a^{n/m} + b^{n/m}) = \frac{1}{n} \sum_{m|n} \mu(n/m) (a^m + b^m).$$

Remark 5.1. The numbers $w_n(G)$ are given by the formula

$$w_n(G) = \frac{1}{n} \sum_{m|n} \mu(n/m) \left[\sum_{0 \leq i \leq [m/2]} (-1)^i \frac{m}{m-i} \binom{m-i}{i} d^{m-2i} \right].$$

(See [La2, Proof of Proposition 4].)

Proposition 5.2. *If $n = p^k m$ with $(m, p) = 1$, then*

$$c_n(G) = w_m(G) + w_{pm}(G) + \dots + w_{p^k m}(G).$$

Example 5.3. Let G be a Demushkin pro- p -group of finite rank d . We have

$$\begin{aligned} c_1(G) &= d, \\ c_2(G) &= \begin{cases} \frac{d^2-d-2}{2} & \text{if } p \neq 2, \\ \frac{d^2+d-2}{2} & \text{if } p = 2, \end{cases} \\ c_3(G) &= \begin{cases} \frac{d^3-4d}{3} & \text{if } p \neq 3, \\ \frac{d^3-d}{3} & \text{if } p = 3, \end{cases} \\ c_4(G) &= \begin{cases} \frac{d^4-5d^2+4}{4} & \text{if } p \neq 2, \\ \frac{d^4-3d^2+2d}{4} & \text{if } p = 2, \end{cases} \\ c_5(G) &= \begin{cases} \frac{d^5-5d^3+4d}{5} & \text{if } p \neq 5, \\ \frac{d^5-5d^3+9d}{5} & \text{if } p = 5. \end{cases} \end{aligned}$$

Observe that our numbers $c_n(G)$, $n = 1, 2, \dots$, also detect the minimal numbers of generators of $G_{(n)}$. Indeed by the remarkable result of I. V. Andožskii and independently by J. Dummit and J. Labute for each open subgroup T of the Demushkin group G , we have the following expression for the minimal number of generators $d(T)$ of T :

$$d(T) = [G : T](d(G) - 2) + 2.$$

(See [NSW, Theorem 3.9.15].) Therefore

$$d_n(G) := d(G_{(n)}) = p^{\sum_{i=1}^{n-1} c_i(G)} (d - 2) + 2.$$

From now on we assume that $G = F / \langle r \rangle$, where F is a free pro- p -group on generators x_1, x_2, \dots, x_d , and

$$r = [x_1, x_2][x_3, x_4] \cdots [x_{d-1}, x_d].$$

Then we extract from [La2] the following fact.

Lemma 5.4. *For every n , $w_n(G) = \text{rank}_{\mathbb{Z}_p} G_n / G_{n+1}$.*

Proof. This follows from [La2, Theorem and proof of Proposition 4]. (Although [La2] only treats abstract discrete groups, his results are also true for pro- p -groups with virtually the same proofs; one only has to replace \mathbb{Z} by \mathbb{Z}_p , subgroups by closed subgroups, and group rings by completed group rings.) \square

Corollary 5.5. *Assume that for each n , B_n represents a \mathbb{Z}_p -basis of G_n / G_{n+1} . Let us write $n = p^k m$ with $(m, p) = 1$. Then a basis of the \mathbb{F}_p -vector space $G_{(n)} / G_{(n+1)}$ can be represented by the following set*

$$B_m^{p^k} \sqcup B_{pm}^{p^{k-1}} \sqcup \cdots \sqcup B_{p^{k-1}m}^p \sqcup B_n.$$

6. SOME OTHER GROUPS

6.1. Free products of a finite number of Demushkin groups and free pro- p -groups.

Let G be a free pro- p product of r Demushkin groups of ranks d_1, \dots, d_r , and of a free pro- p -group of rank e . The Hilbert-Poincaré series of $\text{gr}(\mathbb{F}_p[[G]])$ is

$$P_{\text{gr}(\mathbb{F}_p[[G]])}(t) = \frac{1}{1 - (d_1 + \dots + d_r + e)t + rt^2} =: \frac{1}{(1 - at)(1 - bt)}.$$

We define the sequence $w_n(G), n = 1, 2, \dots$ by

$$w_n(G) = \frac{1}{n} \sum_{m|n} \mu(m)(a^{n/m} + b^{n/m}) = \frac{1}{n} \sum_{m|n} \mu(n/m)(a^m + b^m).$$

Proposition 6.1. *If $n = p^k m$ with $(m, p) = 1$, then*

$$c_n(G) = w_m(G) + w_{pm}(G) + \dots + w_{p^k m}(G).$$

6.2. A free product of a cyclic group of order 2 and a free pro-2-group. We first consider the case of $p = 2$ because this is the case of interest in Galois theory of 2-extensions, and because this case is a bit simpler than the general case of any prime p . This latter case will be covered in the next subsection.

Let $G = C_2 * S$ be a free pro-2 product of the cyclic group C_2 of order 2 and a free pro-2-group of rank d . The Hilbert-Poincaré series of $\text{gr}(\mathbb{F}_2[[G]])$ is

$$P_{\text{gr}(\mathbb{F}_2[[G]])}(t) = \left(\frac{1}{1+t} - dt \right)^{-1} = \frac{1+t}{1-dt-dt^2} =: \frac{1+t}{(1-at)(1-bt)}.$$

We define the sequence $w_n(G), n = 1, 2, \dots$ by

$$w_n(G) = \frac{1}{n} \sum_{m|n} \mu(n/m)(a^m + b^m - (-1)^m).$$

Proposition 6.2. *If $n = 2^k m$ with $(m, 2) = 1$, then*

$$c_n(G) = w_m(G) + w_{pm}(G) + \dots + w_{2^k m}(G).$$

6.3. A free product of a cyclic group of order p and a free pro- p -group. Let $G = C_p * S$ be a free pro- p product of the cyclic group C_p of order p , and a free pro- p -group of rank d . We shall find a formula for $c_n(G)$. The Hilbert-Poincaré series of $\text{gr}(\mathbb{F}_p[[G]])$ is

$$P_{\text{gr}(\mathbb{F}_p[[G]])}(t) = \frac{1 + t + \dots + t^{p-1}}{1 - dt - dt^2 - \dots - dt^p} =: \frac{(1 - \zeta_1 t) \dots (1 - \zeta_{p-1} t)}{(1 - a_1 t) \dots (1 - a_p t)}.$$

We define the sequence $w_n(G), n = 1, 2, \dots$ by

$$w_n(G) = \frac{1}{n} \sum_{m|n} \mu(n/m)(a_1^m + \dots + a_p^m - (\zeta_1^m + \dots + \zeta_{p-1}^m)).$$

Proposition 6.3. *If $n = p^k m$ with $(m, p) = 1$, then*

$$c_n(G) = w_m(G) + w_{pm}(G) + \cdots + w_{p^k m}(G).$$

Remark 6.4. Note that

$$\xi_1^n + \cdots + \xi_{p-1}^n = \begin{cases} -1 & \text{if } (n, p) = 1, \\ p-1 & \text{if } p \mid n. \end{cases}$$

We shall compute $a_1^n + \cdots + a_p^n$. From

$$\frac{1}{(1 - a_1 t) \cdots (1 - a_p t)} = \frac{1}{1 - (dt + dt^2 + \cdots + dt^p)},$$

taking the logarithms of both sides, we obtain

$$\begin{aligned} \sum_{n \geq 1} \frac{1}{n} (a_1^n + \cdots + a_p^n) t^n &= \sum_{n \geq 1} \frac{1}{n} (dt + dt^2 + \cdots + dt^p)^n \\ &= \sum_{n \geq 1} \frac{1}{n} \sum_{\substack{k_1 + \cdots + k_p = n, \\ k_i \geq 0}} \binom{n}{k_1, \dots, k_p} (dt)^{k_1} (dt^2)^{k_2} \cdots (dt^p)^{k_p} \\ &= \sum_{\substack{M \\ k_1 + 2k_2 + \cdots + pk_p = M, \\ k_i \geq 0}} \left[\frac{1}{M - k_2 - \cdots - (p-1)k_p} \binom{M - k_2 - \cdots - (p-1)k_p}{k_1, \dots, k_p} d^{M - k_2 - \cdots - (p-1)k_p} \right] t^M. \end{aligned}$$

Finally comparing the coefficients of t^n gives us the required formula for $a_1^n + \cdots + a_p^n$,

$$\begin{aligned} a_1^n + \cdots + a_p^n &= \sum_{\substack{k_1 + 2k_2 + \cdots + pk_p = n, \\ k_i \geq 0}} \frac{n}{n - k_2 - \cdots - (p-1)k_p} \binom{n - k_2 - \cdots - (p-1)k_p}{k_1, \dots, k_p} d^{n - k_2 - \cdots - (p-1)k_p}. \end{aligned}$$

REFERENCES

- [Be1] E. Becker, *Euklidische Körper und euklidische Hüllen von Körpern*, J. Reine Angew. Math. 268/269 (1974), 41-52.
- [Be2] E. Becker, *Hereditarily-Pythagorean fields and orderings of higher level*, Issue 29 of Monografias de matemática, IMPA Lecture Notes (1978).
- [CEM] S. K. Chebolu, I. Efrat and J. Mináč, *Quotients of absolute Galois groups which determine the entire Galois cohomology*, Math. Ann. 352 (2012), no. 1, 205-221.
- [De1] S. P. Demushkin, *The group of the maximum p -extension of a local field* (Russian), Izv. Akad. Nauk. SSSR Ser. Mat. 25 (1961), 329-346.
- [De2] S. P. Demushkin, *On 2-extensions of a local field* (Russian), Mat. Sibirsk Z. 4 (1963), 951-955.
- [DDMS] J. D. Dixon, M. P. F. Du Sautoy, A. Mann and D. Segal, *Analytic pro- p groups*, second edition, Cambridge Studies in Advanced Mathematics, 61, Cambridge University Press, Cambridge, 1999.

- [Ef1] I. Efrat, *The Zassenhaus filtration, Massey products, and representations of profinite groups*, Adv. Math. 263 (2014), 389-411.
- [Ef2] I. Efrat, *Filtrations of free groups as intersections*, Arch. Math. (Basel) 103 (2014), 411-420.
- [EH] I. Efrat and D. Haran, *On Galois groups over Pythagorean and semi-real closed fields*, Israel J. Math. 85 (1994), no. 1-3, 57-78.
- [EM] I. Efrat and J. Mináč, *Galois groups and cohomological functors*, arXiv:1103.1508v1, to appear in Trans. Amer. Math. Soc.
- [Er] M. Ershov, *Kazhdan quotients of Golod-Shafarevich groups*, Proc. Lond. Math. Soc. (3) 102 (2011), no. 4, 599-636.
- [Fo] P. Forré, *Strongly free sequences and pro- p -groups of cohomological dimension 2*, J. Reine Angew. Math. 658 (2011), 173-192.
- [Gä] J. Gärtner, *Mild pro- p -groups with trivial cup product*, PhD thesis (2011), Universität Heidelberg.
- [Ha] M. Hall, Jr., *A basis for free Lie rings and higher commutators in free groups*, Proc. Amer. Math. Soc., 1 (1950), 575-581.
- [Har] D. Haran, *Closed subgroups of $G(\mathbb{Q})$ with involutions*, J. Algebra 129 (1990), no. 2, 393-411.
- [Hart] M. Hartl, *On Fox and augmentation quotients of semidirect products*, J. Algebra 324 (2010), no. 12, 3276-3307.
- [Ko] H. Koch, *Galois theory of p -extensions*, Springer Monographs in Mathematics (2001).
- [Li] A. I. Lichtman, *On Lie algebras of free products of groups*, J. Pure Appl. Algebra 18 (1980), no. 1, 67-74.
- [La1] J. Labute, *Classification of Demushkin groups*, Canad. J. Math. 19 (1966), 106-132.
- [La2] J. Labute, *On the descending central series of groups with a single defining relation*, J. Algebra 14 (1970), 16-23.
- [La3] J. Labute, *Mild pro- p -groups and Galois groups of p -extensions of \mathbb{Q}* , J. Reine Angew. Math. 596 (2006), 155-182.
- [LM] J. Labute and J. Mináč, *Mild pro-2 groups and 2-extensions of \mathbb{Q} with restricted ramification*, J. Algebra 332 (2011), 136-158.
- [Lam] T. Y. Lam, *Orderings, valuations and quadratic forms*, CBMS Regional Conference Series in Mathematics 52, American Mathematical Society, 1983.
- [Laz] M. Lazard, *Sur les groupes nilpotents et les anneaux de Lie*, Ann. Sci. E. N. S. 71 (1954), 101-190.
- [Le] J.-M. Lemaire, *Algèbres connexes et homologie des espaces de lacets*, Lecture Notes in Mathematics 422, Springer-Verlag, Berlin, 1974.
- [Mi] J. Mináč, *Galois groups of some 2-extensions of ordered fields*, C. R. Math. Rep. Acad. Sci. Canada 8 (1986), no. 2, 103-108.
- [MS1] J. Mináč and M. Spira, *Formally real fields, Pythagorean fields, C -fields and W -groups*, Math. Z. 205 (1990), no. 4, 519-530.
- [MS2] J. Mináč and M. Spira, *Witt rings and Galois groups*, Ann. of Math. (2) 144 (1996), no. 1, 35-60.
- [MT] J. Mináč and N. D. Tân, *Triple Massey products and Galois theory*, to appear in J. Eur. Math. Soc.
- [MTE] J. Mináč and N. D. Tân, *The Kernel Unipotent Conjecture and Massey products on an odd rigid field* (with an appendix by I. Efrat, J. Mináč and N. D. Tân), Adv. Math. 273 (2015) 242-270.
- [NSW] J. Neukirch, A. Schmidt and K. Wingberg, *Cohomology of number fields*, second edition, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], 323, Springer-Verlag, Berlin, 2008.
- [PP] A. Polishchuk and L. Positselski, *Quadratic algebras*, University Lecture Series, 37, American Mathematical Society, Providence, RI, 2005.
- [Qu] D. G. Quillen, *On the associated graded ring of a group ring*, J. Algebra 10 (1968), 411-418.
- [Sha] I. R. Shafarevich, *On p -extensions* (Russian), Math. Sb. 20 (1947), 351-363.
- [Se1] J.-P. Serre, *Structures de certains pro- p -groups*, Sémin. Bourbaki, exposé 252, (1962/63).

- [Se2] J.-P. Serre, *Galois cohomology*, Corr. 2 printing; Springer 2002 (Springer Monographs in Mathematics).
- [Vo] D. Vogel, *On the Galois group of 2-extensions with restricted ramification*, J. Reine Angew. Math. 581 (2005), 117-150.
- [Wa] R. Ware, *When are Witt rings group rings? II.*, Pacific J. Math. 76, no. 2 (1978), 541-564.
- [Zas] H. Zassenhaus, *Ein Verfahren, jeder endlichen p -Gruppe einen Lie-Ring mit der Characteristic p zuzuordnen*, Abh. Mat. Sem. Univ. Hamburg 13 (1940) 200-207.

DEPARTMENT OF MATHEMATICS, WESTERN UNIVERSITY, LONDON, ONTARIO, CANADA N6A 5B7
E-mail address: minac@uwo.ca

DEPARTMENT OF MATHEMATICS, WESTERN UNIVERSITY, LONDON, ONTARIO, CANADA N6A 5B7
E-mail address: mrogelst@uwo.ca

DEPARTMENT OF MATHEMATICS, WESTERN UNIVERSITY, LONDON, ONTARIO, CANADA N6A 5B7
AND INSTITUTE OF MATHEMATICS, VIETNAM ACADEMY OF SCIENCE AND TECHNOLOGY, 18 HOANG
QUOC VIET, 10307, HANOI - VIETNAM
E-mail address: dnguy25@uwo.ca